AMENDMENT AND RESPONSE UNDER 37 C.F.R § 1.111
Serial Number:10/585,517
Filing Date: July 10, 2006
Title: DETECTING RELAYED COMMUNICATIONS

Page 2
Dkt: 2043.561US1

## IN THE CLAIMS

Please cancel claims 37, 39, and 41.

Please amend the claims as follows:

1.    (Currently Amended) A method of determining whether a potential relay device is a relay device, the method comprising:

>    receiving a communication from the potential relay device, the communication comprising a first information element and a second information element, wherein the potential relay device is an original source of said second information element;

>    identifying a feature of an original source of said first information element, the feature of the original source including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source;

>    identifying a feature of the potential relay device, the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

>    determining, using a relay detection system implemented at least in part in hardware, that the feature of the original source of said first information element and the feature of the potential relay device are features unlikely to relate to a single device, said determining being indicative that the potential relay device is a relay device.

2.    (Original) The method of claim 1 wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay.

AMENDMENT AND RESPONSE UNDER 37 C.F.R § 1.111
Serial Number:10/585,517
Filing Date: July 10, 2006
Title: DETECTING RELAYED COMMUNICATIONS

Page 3
Dkt: 2043.561US1

3.     (Previously Presented) The method of claim 2 wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a NA T device.

4.     (Previously Presented) The method of claim 1 wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL.

5.     (Original) The method of claim 1 wherein said first information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL.

6.     (Canceled)

7.     (Previously Presented) The method of claim 1 wherein said first and said second information elements are sent in two different layers of a protocol stack.

8.     (Canceled)

9.     (Previously Presented) The method of claim 1 wherein said stage of determining further comprises:

        comparing said feature of an original source of said first information element with said
            feature of the potential relay device.

10.    (Previously Presented) The method of claim 1 further comprising:

        obtaining a parameter indicative of said feature of an original source of said first
            information element; and

        obtaining a parameter indicative of said feature of the potential relay device.

11.     (Previously Presented) The method of claim 1 wherein said stage of determining further comprises:

        considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered.

12.     (Previously Presented) The method of claim 1 further comprising:

        obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device.

13.     (Original) The method of claim 12, wherein said stage of determining includes analyzing said parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device.

14.     (Original) The method of claim 12 wherein said parameter is obtained from at least one of said first information element and said second information element.

15.     (Previously Presented) The method of claim 1 further comprising:

        sending an outgoing communication to at least one of said original source of said first information element and the potential relay device; and

        receiving a third information element from said at least one of said original source of said first information element and the potential relay device.

16.     (Previously Presented) The method of claim 15, further comprising:

        deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device.

17.     (Previously Presented) The method of claim 15 further comprising:

        verifying that an original source of said third information element is said original source of said first information element.

18.     (Previously Presented) The method of claim 15 further comprising:

verifying that an original source of said third information element is the potential relay
device.

19.     (Original) The method of claim 15 wherein said third information element is selected
from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an
HTTP request, an HTTP response, an HTTP 'Server' header, an IP address, a TCP port, a TCP
Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record.

20.     (Currently Amended) The method of claim 1 wherein at least one of said feature of an
original source of said first information element and said feature of the potential relay device is a
feature related to a device configuration status including an indication of a type of hardware of
the original source or the potential relay device.

21.     (Currently Amended) The method of claim 20 wherein said feature related to a device
configuration status is selected from the group consisting of an operating system type, an
operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP
client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

22.     (Currently Amended) The method of claim 21 wherein said determining includes
examining a parameter indicative of said feature related to a device configuration status.

23.     (Previously Presented) The method of claim 22 wherein said parameter is selected from
the group consisting of an HTTP 'User-Agent' header, an RFC 822 'X-Mailer' header, an RFC
822 'Received' header, an RFC 822 'Date' header, a protocol implementation manner, a TCP/IP
stack fingerprint, an IP address, a TCP port, a TCP initial sequence number, a TCP initial
window, a WHOIS record, and a reverse DNS record.

24.     (Original) The method of claim 1 wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

25.     (Original) The method of claim 24 wherein said feature related to communication performance is selected from the group consisting of a measured communication performance, a measured relative communication performance, and an estimated communication performance.

26.     (Original) The method of claim 24 wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate.

27.     (Original) The method of claim 24 wherein said determining includes examining a parameter indicative of said feature related to communication performance.

28.     (Original) The method of claim 27 wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information.

29.     (Original) The method of claim 28 wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes.

30.     (Original) The method of claim 24, wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device.

31.     (Previously Presented) The method of claim 30, wherein said information about at least one of said original source of said first communication and the potential relay device is selected from the group consisting of a location of a device, a reverse DNS record of a device's IP address, and an administrator of a device.

32.     (Original) The method of claim 1 wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is selected from the group consisting of a subnetwork, an administrator, and a location.

33.     (Currently Amended) The method of claim 32 wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP 'User-Agent' header, an RFC 822 'X-Mailer' header, an RFC 822 'Received' header, an RFC 822 'Date' Header, an IP address, a WHOIS record, and a reverse DNS record[[,]].

34.     (Currently Amended) A method of determining whether a potential relay device is a relay device, the method comprising:

        receiving, from the potential relay device, a first information element and a second information element, wherein the potential relay device is an original source of said second information element;

        analyzing a configuration status of an original source of at least one of said first and said second information elements, said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting;

        identifying a feature of an original source of said first information element, the feature of the original source including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source;

identifying a feature of the potential relay device, the feature of the potential relay device
including a device configuration status of the potential relay device, the device
configuration status including an indication of a type of software installed on the
potential relay device; and

determining, using a relay detection system, whether the feature of the original source of
said first information element and the feature of the potential relay device are features
unlikely to relate to a single device.

35.     (Currently Amended) A method of determining whether a potential relay device is a relay
device, the method comprising:

receiving, from the potential relay device, a first information element and a second
information element, wherein the potential relay device is an original source of said
second information element;

analyzing, using a relay detection system, a feature related to communication
performance of an original source of at least one of said first and said second
information elements;

identifying a feature of an original source of said first information element, the feature of
the original source including communication performance of the original source, the
feature of the original source also including a device configuration status of the
original source;

identifying a feature of the potential relay device, the feature of the potential relay device
including communication performance of the potential relay device, the feature of the
potential relay device also including a device configuration status of the potential
relay device; and

determining, using a relay detection system, whether the feature of the original source of
said first information element and the feature of the potential relay device are features
unlikely to relate to a single device.

36.     (Original) The method of claim 35, wherein said feature related to communication
performance is selected from the group consisting of a latency of communication, a latency of an

incoming communication, a latency of an outgoing communication, a round trip time of a
communication, a communication rate, an incoming communication rate, an outgoing
communication rate, a maximum communication rate, an incoming maximum communication
rate, and an outgoing maximum communication rate.

37.    (Canceled)

38.    (Currently Amended) A method of determining whether a potential relay device is a relay
device, the method comprising:
      receiving, from the potential relay device, a first information element and a second
          information element;
      identifying a feature of an original source of said first information element, the feature of
          the original source of said first information element including a device configuration
          status of the original source of said first information element, the device configuration
          status including an indication of a type of software installed on the original source of
          said first information element;
      identifying a feature of an original source of said second information element, the feature
          of the original source of said second information element including a device
          configuration status of the original source of said second information element, the
          device configuration status including an indication of a type of software installed on
          the original source of said second information element; and
      determining, using a relay detection system, that  the feature of the original source of said
          first information element and the feature of the original source of said second
          information element are features unlikely to relate to a single device, said determining
          being indicative that the potential relay device is a relay device.

39. – 42.    (Canceled)

43.    (Currently Amended) A method of determining whether a potential relay device is a relay
device, the method comprising:

AMENDMENT AND RESPONSE UNDER 37 C.F.R § 1.111          Page 10
Serial Number:10/585,517          Dkt: 2043.561US1
Filing Date: July 10, 2006
Title: DETECTING RELAYED COMMUNICATIONS

identifying a feature of an original source of a first information element, the feature of the original source including a device configuration status of the original source, the device configuration status including an indication of a type of software installed on the original source;

identifying a feature of the potential relay device that transmitted the first information element and a second information element, the potential relay device being the original source of the second information element, the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

determining, using a relay detection system, whether a feature of an original source of a first information element and a feature of the potential relay device are features unlikely to relate to a single device, wherein a positive result of said determining is indicative that the potential relay device is a relay device.

44. (Currently Amended) A system, implemented at least in part in hardware, to determine whether a potential relay device is a relay device, the system comprising:

a processor;

a feature database in data communication with the processor;

an information element receiver, executable by the processor, to receive information elements from a plurality of devices including an information source device and the potential relay device;

a feature discovery module, executable by the processor, to identify at least one of a feature of the information source device and a feature of the potential relay device, the feature of the information source device including a device configuration status of the information source device, the device configuration status including an indication of a type of software installed on the information source device, the feature of the potential relay device including a device configuration status of the potential relay device, the device configuration status including an indication of a type of software installed on the potential relay device; and

a feature incompatibility analyzer, ~~using a~~ executable by the processor and in data
communication with the feature database, to determine whether the feature of said
information source device and the feature of the potential relay device are features
unlikely to relate to a single device.

45.     (Canceled)

46.     (Currently Amended) The system of claim 44, wherein [[said]] the information element
receiver is further configured to receive information elements from a monitored host.

47.     (Currently Amended) The system of claim 44, ~~wherein~~ further comprising:
an outgoing information element sender executable by the processor.

48.     (Currently Amended) The system of claim 44, further comprising:
        a parameter obtainer, executable by the processor, to obtain ~~for obtaining~~ at least one
                parameter selected from the group consisting of a parameter indicative of a feature of
                an information source device, a parameter indicative of a feature of the potential relay
                device, and a parameter indicative of whether a feature of said information source
                device and a feature of said potential relay device are features unlikely to relate to a
                single device.

49.     (Currently Amended) The system of claim 44, ~~further comprising:a~~ wherein the feature
database for storing a map between pairs of features and data indicative of whether said pairs of
features are incompatible features.

50.     (Currently Amended) A computer-readable non-transitory storage medium comprising
instructions, which when executed by a computer cause the computer to ~~perform operations
comprising~~:

receive, from the potential relay device, a first information element and a second
information element, wherein the potential relay device is an original source of said
second information element;

identify a feature of an original source of said first information element, the feature of the
original source including a device configuration status of the original source, the
device configuration status including an indication of a type of software installed on
the original source;

identify a feature of said potential relay device, the feature of the potential relay device
including a device configuration status of the potential relay device, the device
configuration status including an indication of a type of software installed on the
potential relay device; and

determine whether the feature of the original source of said first information element and
the feature of said potential relay device are features unlikely to relate to a single
device, wherein a positive result of said determining is indicative that said potential
relay device is a relay device.